SSS:NDB
F. #2016R00536

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA

- against - 16-CR-191 (PKC)

YANG KIM,
also known as "Andrew Kim,"

Defendant.

----------X

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS

ROBERT L. CAPERS
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

Nomi D. Berenson
Assistant U.S. Attorney
(Of Counsel)

TABLE OF CONTENTS

PRELIMINARY STATEMENT

Defendant Yang Kim, also known as "Andrew Kim," is charged in a two-count indictment with receipt and possession of child pornography. The charges arise out of an investigation by the Federal Bureau of Investigation ("FBI") into Playpen, a website through which registered users, like the defendant, regularly accessed child pornography.

Playpen operated on the anonymous Internet network Tor, which is designed to allow users, such as the defendant, to access websites without revealing their Internet Protocol ("IP") addresses. In February 2015, the FBI sought and obtained a warrant from the United States District Court for the Eastern District of Virginia to monitor user communications and to deploy a Network Investigative Technique ("NIT") on the site, which it did for a two-week period between February 20, 2015, and March 4, 2015 (the "NIT Warrant"). The purpose of the NIT was to identify the otherwise anonymous users of Playpen.

On February 14, 2017, the defendant filed a motion to suppress all of the evidence resulting from the NIT, arguing that the NIT Warrant violated the Fourth Amendment and Federal Rule of Criminal Procedure 41 ("Rule 41"). (ECF Dkt. No. 33, hereinafter "Def. Br.") Specifically, the defendant argues that (i) the NIT constituted a search of the defendant's computer; (ii) the NIT Warrant violated Rule 41 because it authorized a search outside of the district in which the warrant was issued; and (iii) to the extent the NIT Warrant violated Rule 41, the violation was of a constitutional magnitude that prejudiced the defendant and thus warrants exclusion of all of the evidence.

The defendant's arguments are without merit. First, the NIT Warrant complied with Rule 41 because it was a tracking device under Rule 41(b)(4). Second, even if

the NIT Warrant was issued in violation of Rule 41, the violation was technical and does not warrant suppression because the defendant cannot show either prejudice or a deliberate disregard of the rule. Third, if the NIT Warrant was defective, the good-faith exception to the warrant requirement would apply. The negligible, if any, benefit of deterrence in this case would simply not offset the significant costs to society and the justice system. The exclusionary rule is a remedy of last resort, applied only where it results in appreciable deterrence of flagrant, culpable law enforcement misconduct. Here, the error, if there were one, was made by the magistrate judge, not the FBI, making suppression an especially ineffective remedy. Finally, public policy does not support suppression in this case. Faced with the scourge of child exploitation proliferating in the shadows of the dark web, the FBI devised the NIT to track down and apprehend anonymous Playpen users. The FBI detailed its Playpen investigation and the utility of the NIT in an affidavit, presented it to a magistrate judge in the district where the website was located and the NIT would be deployed, obtained judicial authorization for the search, and executed the NIT according to the warrant's terms. Therefore, the agents reasonably relied on it. Allowing the defendant to escape prosecution because a judge allegedly made a non-constitutional, rule-based mistake offends basic concepts of justice and should not be countenanced.

As the Court is aware, because the execution of the NIT Warrant led to the identification of hundreds of Playpen users located across the country, including several in this district, see United States v. Uskokovic, 15-CR-351 (PKC), United States v. Palaniappan, 15-CR-485 (FB), and United States v. Schreiber, 15-CR-377 (ENV), many defendants charged with child exploitation offenses as a result of the NIT Warrant have filed motions to suppress evidence on the same grounds raised by the instant motion. The

overwhelming majority of district courts throughout the country – thirty-nine of forty-three – have denied such motions. As we show below, the defendant's arguments are without merit.

BACKGROUND[1]

Playpen[2] was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography. Playpen operated on an anonymous network available to Internet users known as "Tor." (Ex. A, Macfarlane Aff. ¶¶ 6-7.) Because of the way Tor routes communications through other computers, traditional IP-address-based identification techniques used to investigate online crimes are not viable and law enforcement authorities cannot use traditional investigative strategies to trace a user's IP address and thereby locate and identify users of Tor websites like Playpen. (Id. ¶ 8.)

After executing a court-authorized search, the FBI seized the Playpen server. (Id. ¶ 28.) Rather than merely shut Playpen down, which would have made it impossible to identify and apprehend its users, the FBI then sought and obtained court approval from the United States District Court for the Eastern District of Virginia to monitor user communications and to deploy a NIT on the site, which it did for two weeks between February 20, 2015, and March 4, 2015. (Ex. B, NIT Warrant.) The operation of the NIT was described in the application for the warrant authorizing its use as follows:

---

[1] Because the Court is already familiar with many of the facts underlying the Playpen investigation from prior briefing in this case (ECF Dkt. No. 31), as well as similar briefing in Uskokovic (15-CR-351, ECF Dkt. No. 33), this memorandum only includes those facts that are most relevant to the defendant's motion to suppress.

[2] Playpen is referred to as the "TARGET WEBSITE" in the NIT Warrant and supporting affidavit, attached as Exhibits A and B, and as "Website A" in the Complaint, ECF Docket No. 1.

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, [Playpen] would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from [Playpen], the 3instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government.

(Id. ¶ 33.) Specifically, the NIT would reveal to the government seven items, chiefly the activating computer's IP address. (Id. ¶ 34.) The warrant application explained the nature of Playpen, the investigative difficulties presented by Playpen users' use of the Tor network, the operation of the NIT, and the fact that the NIT could cause activating computers to disclose the seven pieces of information noted above. (See generally Ex. A). On February 20, 2015, the Honorable Theresa Carroll Buchanan, a United States Magistrate Judge for the Eastern District of Virginia, signed the warrant.

Deployment of the NIT Warrant revealed that a Playpen user with the username "zzzzpppp" had actively logged into Playpen for a total of 2 hours and 55 minutes between November 14, 2014, and March 3, 2015. (See ECF Dkt. No. 1, Compl. ¶ 5.) The NIT acquired the IP address of the user's computer, which was registered to an apartment in Queens, New York. (Id. ¶ 6.) Further investigation revealed that, subsequent to March 3, 2015, the residents of that apartment moved to another apartment in Queens. (Id.)

On or about December 22, 2015, FBI agents went to the second apartment, where the residents whose IP address accessed Playpen lived, and conducted a voluntary interview of the defendant. (Id. ¶ 7.) The defendant was advised of the identities of the interviewing agents and the nature of the interview and that he was not under arrest and could end the interview at any time. (Id.) The defendant admitted to viewing child

pornography for approximately two and one-half years, and he further stated that he had visited Playpen and that his Playpen username was "zzzzpppp." (Id. ¶ 8.) The defendant also provided verbal and written consent for the FBI to search his computer. (Id. ¶ 9.) After reviewing the computer, FBI agents determined that it contained multiple video files and images depicting child pornography. (Id. ¶ 10.)

A grand jury subsequently returned an indictment against the defendant for receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(b)(1), and 2252(a)(4) and 2252(b)(2), respectively.

ARGUMENT

The defendant concedes that the NIT Warrant was issued by a neutral and detached federal magistrate judge who determined that it was supported by probable cause and particularly described the place to be searched and items to be seized. These are the three requirements of the Fourth Amendment. None are in dispute. The defendant essentially complains that the NIT constituted a search of his computer and the NIT Warrant was therefore not authorized in the proper district. The defects the defendant complains of, to the extent that any exist, are not of constitutional magnitude and did not prejudice him. Moreover, the federal agents who executed the NIT Warrant reasonably relied on it and acted in good faith. Thus, suppression is not warranted.

Of the forty-three district courts to have evaluated substantially identical motions to suppress evidence on the ground that the NIT Warrant was unlawful, thirty-nine have denied suppression. At least twelve of these courts have concluded that the NIT

Warrant was properly authorized pursuant to Rule 41(b)(4).[3] Twenty-five courts have determined that although the NIT Warrant was not authorized by Rule 41(b), any violation was non-constitutional and non-prejudicial, and the evidence was admissible under the good-

[3] See United States v. Bee, No. 16-CR-002, 2017 WL 424905 (W.D. Mo. Jan. 13, 2017) (report and recommendation); United States v. Sullivan, No. 16-CR-270, 2017 WL 201332 (N.D. Ohio Jan. 18, 2017); United States v. McLamb, No. 16-CR-92, 2016 WL 6963046 (E.D. Va. Nov. 28, 2016); United States v. Lough, No. 16-CR-18, 2016 WL 6834003 (N.D. W. Va. Nov. 18, 2016); United States v. Kienast, No. 16-CR-103, 2016 WL 6683481 (E.D. Wis. Nov. 14, 2016); United States v. Mascetti, No. 16-CR-308 (M.D.N.C. Oct. 24, 2016) (attached as Ex. C); United States v. Johnson, No. 15-CR-340, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); United States v. Smith, No. 15-CR-467 (S.D. Tex. Sep. 28, 2016) (attached as Ex. D); United States v. Jean, No. 15-CR-50087, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); United States v. Eure, No. 16-CR-43, 2016 WL 4059663 (E.D. Va. July 28, 2016); United States v. Darby, No. 16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016); United States v. Matish, 193 F.Supp.3d 585 (E.D. Va. 2016); see also United States v. Laurita, No. 13-CR-07, 2016 WL 4179365 (D. Neb. Aug. 5, 2016) (finding similar 2012 NIT warrant deployed on Tor network child pornography website properly authorized under Rule 41(b)(4)).

faith exception to the exclusionary rule.[4] Only four courts have found that the issuing magistrate judge lacked jurisdiction to issue the NIT Warrant and that suppression of evidence was required.[5]

I. THE NIT WARRANT COMPLIED WITH RULE 41

Rule 41(b)(4) authorized the magistrate judge in the Eastern District of Virginia to issue a warrant to install the NIT on the government-controlled Playpen server

---

[4] See United States v. Deichert, No. 16-CR-201, 2017 WL 398370 (E.D. N.C. Jan. 28, 2017); United States v. Tran, No. 16-CR-10010, 2016 WL 7468005, at *6 (D. Mass. Dec. 28, 2016); United States v. Dzwonczyk, No. 15-CR-3134, 2016 WL 7428390, at *1 (D. Neb. Dec. 23, 2016); United States v. Vortman, No. 16-CR-210, 2016 WL 7324987 (N.D. Ca. Dec.16, 2016); United States v. Hammond, No. 16-CR-102, 2016 WL 7157762, at *5 (N.D. Cal. Dec. 8, 2016); United States v. Duncan, No. 15-CR-414, 2016 WL 7131475 (D. Or. Dec. 6, 2016); United States v. Owens, No. 16-CR-38, 2016 WL 7053195 (E.D. Wisc. Dec. 5, 2016); United States v. Tippens et. al., No. 16-CR-5110 (W.D. Wa. Nov. 30, 2016) (attached as Ex. E); United States v. Stepus, No. 15-CR-30028, 2016 WL 6518427 (D. Mass. Oct. 28, 2016); United States v. Libbey-Tipton, No. 16-CR-236 (N.D. Ohio Oct. 19, 2016) (attached as Ex. F); United States v. Allain, No. 15-CR-10251, 2016 WL 5660452 (D. Mass. Sep. 29, 2016); United States v. Anzalone, No. 15-CR-10347, 2016 WL 5339723 (D. Mass. Sept. 22, 2016); United States v. Broy, No. 16-CR-10030, 2016 WL 5172853 (C.D. Il. Sept. 21, 2016) ; United States v. Ammons, No. 16-CR-00011, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); United States v. Knowles, No. 15-CR-875, 2016 WL 6952109 (D.S.C. Sep. 14, 2016); United States v. Scarbrough, No. 16-CR-35, 2016 WL 5900152 (E.D. Tenn. Oct. 11, 2016); United States v. Torres, No. 16-CR-285, 2016 WL 4821223 (W.D. Tex. Sep. 9, 2016); United States v. Henderson, No. 15-CR-565, 2016 WL 4549108 (N.D. Cal. Sep. 1, 2016); United States v. Adams, No. 16-CR-11, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016); United States v. Acevedo-Lemus, No. 15-CR-137, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); United States v. Rivera, No. 15-CR-266 (E.D. La. July 20, 2016) (attached as Ex. G); United States v. Werdene, 188 F.Supp.3d 431 (E.D. Pa. 2016); United States v. Epich, No.15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); United States v. Stamper, No. 15-CR-109, 2016 WL 695660 (S.D. Ohio, Feb. 19, 2016); United States v. Michaud, No. 15-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

[5] United States v. Croghan, No. 15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); United States v. Workman, No. 15-CR-397, 2016 WL 5791209 (D. Co. Sept. 6, 2016); United States v. Arterbury, No. 15-CR-182 (N.D. Okla. May 17, 2016) (attached as Ex. H); United States v. Levin, No. CR 15-10271, 2016 WL 2596010 (D. Mass. May 5, 2016).

located within the district, and that warrant properly authorized use of the NIT to track the movement of information—the digital child pornography content requested by users who logged into Playpen's website—as it traveled from the server in the Eastern District of Virginia through the encrypted Tor network to its final destination: the users' activating computers, wherever located. At that point, the NIT caused the activating computers to transmit specified network information back to the government over the open Internet, thus enabling the government to locate and identify the user. See, e.g., Johnson, 2016 WL 6136586, at **3-7 (holding that the NIT Warrant was authorized under Rule 41(b)(4)); Smith, No. 15-CR-467, at 14-15 (same); Jean, 2016 WL 4771096, at **15-17 (same); Eure, 2016 WL 4059663, at *8 (same); Darby, 190 F.Supp.3d 520, 535-37 (same); Matish, 183 F.Supp.3d at 612-13 (same).

A. Rule 41 Should Be Read Broadly and Flexibly

Courts have long read Rule 41 broadly, interpreting it to permit searches that comply with the Fourth Amendment even though not explicitly authorized by the text of the rule. In United States v. New York Telephone Co., 434 U.S. 159, 169 & n.16 (1977), for example, the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" at that time did not include information and that Rule 41 required that a search be conducted within 10 days. The Court explained that Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause," and noted that this flexible reading was bolstered by Rule 57(b), which provided that "[i]f no procedure is

specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." Id. at 169-70 (emphasis added).[6]

Similarly, in United States v. Biasucci, 786 F.2d 504, 509 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986), the Second Circuit affirmed a magistrate judge's issuance of a warrant under Rule 41 to allow for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. See also United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992) (same). As the Second Circuit stated in United States v. Villegas, 899 F.2d 1324, 1334 (2d Cir. 1990),

> Rule 41 does not define the extent of the court's power to issue a search warrant. Obviously the Fourth Amendment long antedated the Federal Rules of Criminal Procedure, which were first adopted in 1944. Given the Fourth Amendment's warrant requirements, and assuming no statutory prohibition, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met.

Stated another way, when presented with a constitutionally valid, and not statutorily prohibited, request for a search warrant, courts are empowered to read the

[6] Rule 57(b) now provides: "A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."

language of Rule 41 broadly in determining whether the requested search falls within its scope.[7]

B. The NIT was a Tracking Device under Rule 41(b)(4)

Rule 41(b)(4) provides that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. The Rule defines "property" to include not only "tangible objects" but also "information." Fed. R. Crim. P. 41(a)(2)(A). A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). Although the term "device" is not more specifically defined in the Rule, it is a word commonly used to describe "[a] thing made or adapted for a particular purpose." Oxford English Dictionary, https://en.oxforddictionaries.com/definition/device (last visited: Mar. 7, 2017).

In a physical tracking device case, investigators may obtain a warrant to install a tracking device in a container holding contraband, and investigators may then determine the location of the container after targets of the investigation carry the container outside the

---

[7] The Supreme Court's flexible approach to Rule 41 vindicates Fourth Amendment interests by encouraging law enforcement authorities to seek a warrant, rather than resorting to warrantless searches justified by claims of exigency; and by allowing magistrate judges to issue warrants for searches that meet the requirements of the Fourth Amendment but may not fit neatly within Rule 41's parameters due to advances in technology. See United States v. Torres, 751 F.2d 875, 880 (7th Cir. 1984) ("[H]olding that federal courts have no power to issue warrants authorizing [an investigative technique] might . . . simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment.").

district. In this case, the NIT functioned in a similar manner, except in the Internet context. Investigators installed the NIT in the Eastern District of Virginia on the server that hosted Playpen. When the defendant logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information from the defendant's computer back to law enforcement authorities. Although this network information was not itself location information, investigators subsequently used this network information to identify and locate the defendant. Applying Rule 41 flexibly, as the Supreme Court has instructed, at least twelve district court decisions have held that the NIT Warrant was properly authorized as a "tracking device."[8]

In his brief, the defendant contends that the NIT was not a tracking device because (i) the NIT does not track the target computer; (ii) the NIT was "installed" on the defendant's computer located in New York, not Virginia; and (iii) the defendant did not control the government-controlled computer. (Def. Br. at 8-9.) These arguments are unavailing.

First, as set forth above, the NIT was designed to follow illegal child pornography content requested by a user who accessed Playpen in the Eastern District of Virginia, through the anonymous Tor network nodes, and back to the user's activating

---

[8] See Bee, 2017 WL 424905; Darby, 190 F.Supp.3d 520; Matish, 193 F.Supp.3d 585; Eure, 2016 WL 4059663 (incorporating Darby, authored by same judge); Jean, 2016 WL 4771096; Smith, No. 15-CR-00467; Johnson, 2016 WL 6136586; Mascetti, No. 16-CR-308; Kienast, 2016 WL 6683481; Lough, 2016 WL 6834003; McLamb, 2016 WL 6963046; Sullivan, 2017 WL 201332; see also Laurita, 2016 WL 4179365 (finding that a similar 2012 NIT warrant deployed on a Tor network child pornography website was properly authorized under the tracking device provision of Rule 41(b)(4)).

computer. At that point, the NIT caused the transmission of the location-identifying information back to the government over the open Internet, thus circumventing Tor's encryption and allowing the government to identify and locate the user. Similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates) back to a government-controlled receiver at pre-determined intervals, the NIT was designed to send location-enabling information (like an actual IP address) back to a government-controlled computer when the illegal child pornography content reached its ultimate destination—the user's activating computer. Thus, although not a physical beeper affixed to a tangible object, the NIT operated as a digital tracking device of intangible information within the meaning of Rule 41(b)(4). See, e.g., Jean, 2016 WL 4771096, at *16 ("[T]he purpose of the NIT was to track the movement of 'property'—which in this case consisted of intangible 'information,' something expressly contemplated by the definition in Rule 41(a)(2)(A).").

Second, the NIT was installed in the Eastern District of Virginia, as required by Rule 41(b)(4), which authorizes a magistrate judge "to issue a warrant to install within the district a tracking device." After being installed in the Eastern District of Virginia, the NIT only moved outside the district after a Playpen user digitally entered the district to retrieve the illegal website content it augmented. Agents deployed the NIT alongside Playpen's digital content on the government-controlled server in the Eastern District of Virginia. (Ex. A at ¶ 32.) This deployment constituted installation of a tracking device under Rule 41, as users then retrieved the NIT from the Playpen server by logging on and downloading information from that server. Any person seeking to access Playpen's child pornography content thus had to make, "in computer language, 'a virtual trip' via the Internet to Virginia,"

where the server was located. E.g., Matish, 193 F.Supp.3d at 621; Smith, Ex. D, at 14-15 (same); Darby, 190 F.Supp.3d at 536 (same). When an individual entered his username and password on the Playpen website, it triggered installation of the NIT; both of these actions occurred in the Eastern District of Virginia. (Ex. A at ¶ 33.) Thus, for purposes of Rule 41's tracking-device provision, the NIT was installed at the location where it was obtained by a Playpen user (the Playpen server in the Eastern District of Virginia), not where the NIT ultimately disclosed the location-identifying information (the user's computer). And like a tangible tracking device, it followed the digital information or "property" obtained from Playpen in Virginia to its destination, namely the defendant's computer in New York, and reported that location back to government agents. See, e.g., Matish, 193 F.Supp.3d at 612-13 (finding that "the [NIT's] installation did not occur on the government-controlled computer but on each individual computer that entered the Eastern District of Virginia when the user logged into Playpen via the Tor network," thus functioning "just as traditional tracking devices do").

Third, the argument that Playpen users never controlled the government-controlled computer misses the mark. As a Playpen user, the defendant logged into the Playpen server and sent commands directing the server to return information to him; the server complied with those commands. That the defendant did not have administrator-level control over the computer server hosting the Playpen website does not mean that he did not control his access to Playpen or its illegal content. Unless and until a user affirmatively logged onto the Playpen website in the Eastern District of Virginia, where the NIT had already been embedded, the NIT could not be deployed. See Jean, 2016 WL 4771096, at *17 (noting that "[i]t is also undisputed that but for [the defendant] electronically travelling in

search of child pornography to the [Playpen server] in Virginia, the NIT could not have been deployed"); Smith, Ex. D, at 14-15 (noting that the defendant caused the NIT's deployment by entering the district via the Internet to avail himself of Playpen's child pornography content).

Finally, Rule 41 has since been revised and now explicitly authorizes a tracking device such as the NIT. See Rule 41(b)(6) ("[A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means.") As noted by at least two courts, the amendment and accompanying memorandum support the conclusion that the amendment sought to clarify Rule 41, not expand its scope. Darby, 190 F.Supp.3d at 536 (stating that the amendment "clarif[ied] the scope of Rule 41(b))"); Smith, Ex. D, at 15 (same). Moreover, by Order dated April 28, 2016, the United States Supreme Court decreed that the amendment to Rule 41 "shall take effect on December 1, 2016, and shall govern in all proceedings in criminal cases thereafter commenced and, insofar as just and practicable, all proceedings then pending." United States Supreme Court Order, Apr. 28, 2016, Oct. Term 2015, https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf (last visited: Mar. 7, 2017) (emphasis added). That pronouncement by the Supreme Court further supports denying the instant motion to suppress. See Acevedo-Lemus, 2016 WL 4208436, at *8 ("It would be strange indeed for the Court to suppress the evidence in this case in the face of a strong signal from the Supreme Court that Rule 41 should explicitly permit the issuance of

warrants like the NIT Warrant."). Thus, if there is no Fourth Amendment issue with this type of warrant now, it follows that there was no Fourth Amendment issue with the NIT Warrant when it was issued in February of 2015.

For these reasons, this Court should join the district court decisions (see page 6, supra, at n.3) holding that Rule 41(b)(4) authorized the issuance of the NIT Warrant.

II. SUPPRESSION IS UNWARRANTED EVEN IF ISSUANCE OF THE NIT WARRANT VIOLATED RULE 41

Even if the issuance of the NIT Warrant did not strictly comply with Rule 41's requirements, suppression is not warranted. The Second Circuit has admonished that "courts should be wary in extending the exclusionary rule in search and seizure cases to violations which are not of constitutional magnitude." United States v. Pangburn, 983 F.2d 449, 455 (2d Cir. 1993) (quoting United States v. Burke, 517 F.2d 377, 386-87 (2d Cir. 1975)). For evidence to be suppressed due to a Rule 41 violation, the Second Circuit requires that a defendant show that "(1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." Id. at 455. Applying this standard, it is clear that there was no prejudice to the defendant. Even if the NIT Warrant was issued without strict adherence to the requirements of Rule 41(b), it fully complied with the Fourth Amendment's warrant requirements that it be issued by a neutral and detached magistrate, supported by probable cause, and sufficiently particular. Further, the defendant has failed to establish that the FBI intentionally or deliberately disregarded Rule 41(b)'s venue provision.

C. Technical Noncompliance with Rule 41(b) Does Not Warrant Exclusion of Evidence

The defendant does not dispute – nor could he – that the NIT Warrant was supported by probable cause, particularly described the place to be searched and items to be seized, and was issued by a neutral and detached magistrate judge. Rather, he argues that the NIT Warrant was "void ab initio" because it was issued in the wrong district. (Def. Br. at 9-12.)

Second Circuit case law makes clear that the "failure of a warrant to conform to provisions of Rule 41 other than those concerned with the constitutional requirements" of the Fourth Amendment will not trigger the exclusionary rule absent a showing of prejudice to the defendant or deliberate and intentional disregard of the Rule. See Burke, 517 F.2d at 385-87; United States v. Dewar, 489 F. Supp. 2d 351, 365 (S.D.N.Y. 2007) (finding suppression to be an inappropriate remedy where a warrant was supported by probable cause and defendants suffered "no prejudice from the technical violation of Rule 41"); see also United States v. Johnson, 660 F.2d 749, 753 (9th Cir. 1981) ("Only a 'fundamental' violation of Rule 41 requires automatic suppression, and a violation is 'fundamental' only where it, in effect, renders the search unconstitutional under traditional fourth amendment standards.").

Although Rule 41(b) sets geographic limits on the territorial authority of magistrate judges to issue search warrants,[9] the Fourth Amendment is silent as to where the magistrate's authority may be exercised. Because the NIT Warrant was issued by a neutral and duly appointed magistrate judge who determined that the warrant was supported by probable cause and particularly described the place to be searched and things to be seized, any violation of Rule 41 was technical and not of constitutional magnitude. See, e.g., Allain, 2016 WL 5660452, at *11 n.8; Werdene, 188 F.Supp.3d at 446 (finding a Rule 41 violation to be nonconstitutional); Matish, 193 F.Supp.3d at 622 ("[A]ny potential Rule 41 violation did not result in a violation of Defendant's constitutional rights, for no warrant was needed."); Michaud, 2016 WL 337263, at *6 (holding that "the NIT Warrant did not fail for constitutional reasons, but rather was the product of a technical violation of Rule 41(b)").

The defendant cites the Second Circuit's decision in United States v. Burke for the proposition that suppression is warranted where (1) the search may not have occurred if Rule 41 had been followed or (2) there is evidence of intentional and deliberate disregard for Rule 41. (Def. Br. at 11-14.) However, in Burke, the Second Circuit considered and rejected

---

[9] The version of Rule 41(b) in effect at the time the NIT Warrant was issued provides that a magistrate judge has authority to issue a warrant (1) to search for and seize "a person or property located within the district;" (2) "if the person or property is located within the district but might move or be moved outside the district before the warrant is executed;" (3) if the magistrate judge sits in a district in which "activities related to terrorism may have occurred;" (4) to install a tracking device within the district, though the magistrate judge may authorize the continued use of the device if the person or object subsequently moves or is moved outside of the district; and (5) where the criminal activities occur in the District of Columbia, any United States territory, or on any land or within any building outside of the country owned by the United States or used by a United States diplomat. Fed. R. Crim. P. 41(b).

a motion to suppress where a warrant failed to specify the time within which the search was to be conducted. The defendant had moved to suppress on that basis and on the basis of two other technical violations of Rule 41. Nevertheless, the Court concluded that there was "no ground at all for thinking that [the issuing judge] would not have been quite as willing to issue a warrant calling for execution . . . within ten days" and there was no evidence of intentional or deliberate disregard of Rule 41. 517 F.2d at 387. For those reasons, Judge Henry Friendly held that "the violations [of Rule 41] . . . were not of sufficient consequence to justify use of the exclusionary rule," id. at 385, and declined even to remand for a hearing. See id. at 387.

The defendant appears to rely on Burke not for its holding but for its description of the former Fifth Circuit's decision in Navarro v. United States, 400 F.2d 315, 316-20 (5th Cir. 1968). In Navarro, the court required suppression of evidence under Rule 41(a) after a Texas city corporation court, not a court of record, issued a warrant at the request of two local police officers and federal agents subsequently executed the warrant. Id. Navarro is, however, no longer good law in the Fifth Circuit. See United States v. McKeever, 905 F.2d 829, 832-33 (5th Cir. 1990) (overruling Navarro in part and declining to reach, though acknowledging, the government's "weighty" arguments that Navarro was wrongly decided); United States v. Comstock, 805 F.2d 1194, 1207 (5th Cir. 1986) ("Plainly, Navarro . . . which considered suppression the automatic consequence of violation of Rule 41(a), can no longer stand" in light of subsequent case law.); see also United States v. Freeman, 897 F.2d 346, 349 (8th Cir. 1990) (recognizing the overruling).

Numerous other courts evaluating violations of analogous Rule 41 provisions have found them to be non-constitutional and denied suppression. For example, courts have

denied motions to suppress evidence where the warrant was issued by an unauthorized individual, see, e.g., United States v. Britt, 959 F.2d 232 (4th Cir. 1992) (unpublished) (per curiam) (assuming that issuance of a warrant by an unauthorized state judge violated Rule 41, "a technical breach of Rule 41, without more, does not mandate suppression of evidence" and since the defendant "has not shown that the search violated fourth amendment principles . . . the exclusion of evidence would be inappropriate"); Comstock, 805 F.2d at 1207 (similar); and where the warrant was requested or executed by an unauthorized individual, see, e.g., United States v. Freeman, 897 F.2d 346, 348 (8th Cir. 1990) (holding that a warrant requested by an individual who was not "a federal law enforcement officer" violated Rule 41, but that suppression was not required because the violation was non-fundamental and non-prejudicial); United States v. Luk, 859 F.2d 667, 673 (9th Cir. 1988); Burke, 517 F.2d at 386-87. Courts also have held, or stated in dicta, that suppression was not required where, as is alleged here, the warrant authorized a search that exceeded Rule 41's territorial limitations. See, e.g., United States v. Berkos, 543 F.3d 392, 396 (7th Cir. 2008) (stating, in dicta, that a violation of Rule 41(b) caused by the issuance of a warrant that authorized a search in another judicial district would not require suppression); United States v. $64,000 in U.S. Currency, 722 F.2d 239, 246 (5th Cir. 1984) (holding that any Rule 41 violation that occurred when a Louisiana judge issued a warrant to search an envelope seized in Utah and then brought to Louisiana did not warrant suppression); United States v. Goff, 681 F.2d 1238, 1240 & n.1 (9th Cir. 1982) (noting that even if a search warrant for items that were not yet in the district violated Rule 41, suppression was not required).

Because the NIT Warrant fully complied with the Fourth Amendment, any alleged Rule 41(b) technical error did not render the warrant unconstitutional.

D. The Defendant Has Failed to Establish Prejudice or Intentional or Deliberate Disregard of Rule 41

Suppression is not warranted on the basis of a technical violation of Rule 41(b) because the defendant has failed to show that he was prejudiced or that the FBI acted intentionally and with deliberate disregard of Rule 41(b).

In support of his claim that he was prejudiced by noncompliance with Rule 41, the defendant makes two arguments. (Def. Br. at 12-14.) First, he argues that he was prejudiced because the NIT Warrant was issued "by an Eastern District of Virginia magistrate judge without power to authorize a search in New York" in other words, he argues that he was prejudiced by a technical violation of Rule 41(b). As the court in Michaud aptly pointed out, such an interpretation "makes no sense, because under that interpretation, all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be. Such an interpretation would defeat the need to analyze prejudice separately from the Rule 41(b) violation." 2016 WL 337263, at **6-7. The NIT Warrant satisfied the Fourth Amendment's probable cause and particularity requirements, and thus, had it been presented to a magistrate judge in the Eastern District of New York, Rule 41(b)(1) would have authorized the same search that actually occurred. Cf. Darby, 190 F.Supp.3d at 536-37 (finding no prejudice because Rule 41(b)(1) authorized search of defendant's computer, located in Eastern District of Virginia); United States v. Ritter, 752 F.2d 435, 441 (9th Cir. 1985) (declining to suppress evidence because there was "no indication that a federal magistrate would have handled the search differently than did the state judge").

The defendant's additional argument that he was prejudiced in some unspecified way because he was not provided timely notice of the NIT Warrant can be summarily rejected. (Def. Br. at 13-14.) First, even if the defendant had not been timely notified, such an error would not violate his Fourth Amendment rights and, for all of the reasons set forth above, would not warrant the remedy of suppression.[10] See McLamb, 2017 WL 243987 (denying motion to suppress NIT Warrant where defense counsel was provided a copy of the warrant four months after expiration of court-authorized delayed-notice period, finding neither prejudice nor deliberate disregard by the government); see also United States v. Welch, 811 F.3d 275, 277 (8th Cir. 2016) (affirming denial of motion to suppress alleging delayed notice violation regarding the NIT Warrant, finding neither prejudice nor deliberate disregard by the government); Pangburn, 983 F.2d 449 (2d Cir. 1993). Additionally, after the NIT Warrant was issued in the Eastern District of Virginia, Magistrate Judge Theresa Carroll Buchannan issued four orders authorizing 90-day extensions of the 30-day notice requirement in the NIT Warrant. The last such order was issued on December 21, 2015.[11] Thus, the defendant's notification on or about March 9, 2016 was within the 90-day period and, therefore, timely. Additionally, the NIT Warrant was publicly available on the internet as early as March 7, 2016. Further, any alleged violation of Rule 41(f) is ministerial in

---

[10] The version of Rule 41(f)(C) in effect when the NIT Warrant was issued provided that the officer executing a warrant must provide a copy of the warrant and "a receipt of the property taken" to the person from whom the property was taken. The Rule has since been amended to state that, in the context of a warrant to use remote access to search electronic storage media, the officer executing the warrant must "make reasonable efforts" to serve the subpoena and receipt.

[11] These orders remain under seal in the Eastern District of Virginia.

nature. The technical violation alleged does not render the search conducted unreasonable, meaning there is no legal basis to suppress any evidence.

The defendant also fails to establish that the FBI acted intentionally and with deliberate disregard of Rule 41(b) and (f).[12] He declares that the alleged violations, and in particular the alleged violation of Rule 41(b), constitute the "intentional[] and deliberate[] disregard" of the Rules, Def. Br. at 14, but he provides no factual support for such a claim. Nor could he. A review of the record in this case demonstrates that the government and the FBI did not act with intentional or deliberate disregard of Rule 41(b) or (f). As the court in Werdene found, the warrant application was "candid about the challenge that the Tor network poses, specifically its ability to mask a user's physical location" and the government did not "mislead the magistrate judge" but fully explained the NIT's "method and scope." 2016 WL 3002376, at *11. The affidavit also specifically stated that the NIT may be deployed against an "activating computer—wherever located." (Ex. A, at ¶ 28.) With regard to timely notice, the defendant cannot deny that the NIT Warrant was publicly available by March 2016. Moreover, there is no reason the FBI would have deliberately delayed notice, as there was nothing to be gained by doing so. Any delay here was not deliberate.

---

[12] In a footnote, the defendant requests the opportunity for additional briefing and a Franks hearing regarding alleged misrepresentations about the Playpen homepage at the time the NIT Warrant was issued. (Def. Br. at 1, n.1.) Although the defendant has not actually briefed his argument, the government notes that nine courts have denied requests for Franks hearings based on what appears to be the same claims alluded to in the defendant's brief. See United States v. Tran, No. CR 16-10010, 2016 WL 7468005, at *6-9 (D. Mass. Dec. 28, 2016); Owens, 2016 WL 7079609, at *6; McLamb, 2016 WL 6963046, at *5, n.4; Allain, 2016 WL 5660452, at *7–8; Anzalone, 2016 WL 5339723, at *8; Eure, 2016 WL 4059663, at *7; Matish, 193 F.Supp.3d at 604-07; Darby, 190 F.Supp.3d at 533-34; Michaud, 2016 WL 337263, at *1, *3 n.1.

Accordingly, as the defendant has shown neither prejudice nor an intentional violation of Rule 41(b), suppression is not warranted.

III. THE GOOD FAITH EXCEPTION APPLIES

Suppression is also unwarranted because agents acted in objectively reasonable reliance on the issuance of the NIT Warrant. Under the good-faith exception to the exclusionary rule, when law enforcement officers act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral and detached magistrate judge, "the marginal or nonexistent benefits produced by suppressing evidence . . . cannot justify the substantial costs of exclusion." United States v. Leon, 468 U.S. 897, 922 (1984). The good-faith exception thus recognizes that "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope . . . there is no police illegality and thus nothing to deter." Id. at 920-21.

Here, any purported defect in the issuance of the NIT Warrant—the absence of authority to issue the warrant under Rule 41(b)—was made by the magistrate judge and not law enforcement authorities. The application in support of the NIT Warrant was thorough, accurately described the NIT, how it would be used, and why it was necessary. Moreover, when the FBI sought judicial approval for the NIT Warrant, it had already received judicial approval to use NITs in other cases. See, e.g., Laurita, 2016 WL 4179365. That district courts evaluating similar motions to suppress have found the NIT Warrant to have complied with Rule 41 underscores the reasonableness of the FBI's deference and reliance on the magistrate judge's determination of her own authority to issue the NIT Warrant. Leon, 468 U.S. at 914 (mandating deference to magistrate judge's decision where "[r]easonable minds" have differed on legal sufficiency of warrant).

As this case falls squarely within the bounds of the good-faith exception to the exclusionary rule, suppression is not warranted.

IV. PUBLIC POLICY AND DETERRENCE FAVOR DENIAL OF THE MOTION

First, for all of the reasons set forth above, the NIT Warrant was authorized by Rule 41 and, even if it were not, it was at most a technical violation that does not merit suppression. Second, the absence of any deterrent benefit from suppression is underscored by the recently enacted amendment to Rule 41(b), which expressly permits magistrate judges to authorize warrants for remote electronic searches like the one at issue. The new rule confirms that the drafters of the Federal Rules intended that the kind of warrant issued here should not be deterred. Third, to the extent there was an error, it was by the magistrate judge, thus leaving no future law enforcement misconduct to deter. Fourth, for the reasons set forth above, there was no law enforcement misconduct: the FBI detailed its investigation and the utility of the NIT in an affidavit; presented it to a magistrate judge in the district where Playpen was located and where the NIT would be deployed; obtained judicial authorization; and executed the NIT according to the warrant's terms. In short, the process worked as it should.[13]

Finally, to the extent there is any marginal deterrent result from suppression, it would not remotely offset the significant costs to society and the justice system. Allowing

---

[13] See Darby, 190 F.Supp.3d at 538 ("The FBI agents in this case did the right thing. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate in support of their search warrant application. They filed the warrant application in the federal district that had the closest connection to the search to be executed . . . The FBI should be applauded for its actions in this case.").

the defendant and other viewers and distributors of child pornography to escape prosecution for the exploitation of children in the shadows of Tor – simply because a judge allegedly made a non-constitutional, rule-based mistake – would be contrary to basic concepts of justice.

CONCLUSION

For the foregoing reasons, the defendant's motion to suppress should be denied in full.

Dated: Brooklyn, New York
March 7, 2017

Respectfully submitted,

ROBERT L. CAPERS
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

By: /s/ Nomi Berenson
Nomi D. Berenson
Assistant United States Attorney
(718) 254-6308